REMARKS

The undersigned thanks Examiner Nguyen for the interview of June 3, 2008. The amendments made herein were discussed during the interview and are based on the specification and drawings of the application, and it was agreed that the amendments distinguish the references of record.

As discussed during the interview, the application describes a computerized methodology which allows personal information (e.g., clinical data) to be used by a web site operator to enhance an anonymous user's use of the web site while maintaining the security and confidentiality of the personal information (e.g.., the web site operator does not have information which would link the personal information to a particular person). In particular, the web site operator would have the web pages of the web site indexed by industry standard medical codes (see page 6 of the application et seq.). The web site would include a user record for each user which also include the industry standard medical codes (see page 7). Thus, the user, when visiting the web site, might be presented with web pages that are paired to his or her medical codes, or his or her searches might be automatically modified to identify web pages which relate to his or her medical history (as defined by the codes), or his or her searches may be modified based on the statistical browsing habits of other user's with similar codes, or by a variety of other mechanisms (see pages 7-8, 24-29, and Figure 7-9 of the application).

Because one aspect of the invention allows for person specific data to be used at a web site, there invention includes a specific mechanism for maintaining the security of the person specific data. For example, the claimed methods assure that the person specific data will not be compromised by the web site operator (or a person that compromises the security of the web site), and individuals that use the web site cannot learn private information about other individuals.

Claims 51-53 are differentiated from Illiff according to the Tables below:

51. A method of transferring personal information of a plurality of users from a first database in which said personal information, including medical information, is identifiable with particular users to a second database associated with a web server in which said personal information is de-identified, said method comprising the steps:	Figure 25a of Iliff shows components of a user computer in a network based embodiment of the MDATA system (see column 6, lines 10-12). Reference to columns 71-73 of Iliff shows that Iliff shows a user being able to interact with one or more servers connected through a common gateway 2104. The user can interact using his computer 2116, phone 2124, a portable PC 2126, a cable box 2128, or satellite dish 2132. What is NOT shown is transferring of identifiable data from a first database to a second database where it is de-identified.
uploading to said second database associated with said web server de-identified personal information, including medical information, of said users from said first database;	This is not shown in Iliff. With reference to Column 74, lines 46-57 of Iliff, it can be seen that the user interacts directly with the MDATA system–i.e., the user logs on, and the system which knows who the patient is obtains data about the patient). At no point does Iliff mention de-identified data being at a second database where the de-identified data is from a first database. The Examiner's reference to charts, audio files, photos, etc. is not on point since this is not de-identified data obtained from a first database.

uploading to said second database from a third database associated with a registration authority server anonymous IDs for each of said users; and	This is not shown in Iliff. In Iliff there is no third database associated with a registration authority that issues annonymous Ids. Rather, with reference to column 35 (cited by the Examiner), Iliff contemplates a simple personal identification number (PIN) number arrangement, where access to the system requires the patient or his assistant to enter a PIN number specific for the patient—In short Iliff shows not anonymous ID being transferred from a third database to the second database which has the de-identified data, AND Iliff does not show the third database being separate from the first database.

indexing said de-identified personal information, including medical information, of said users in said second database by anonymous ID without providing indexing to said first database.	Iliff does not show this feature. The Examiner's reference to Figures 1 and 25a is simply in error. With reference to pages 3 and 4 of the office action, the Examiner is equating a PIN or an AIN (in the case of a patient's assistant) to indexed de-identified data. This is incorrect. If you have a PIN or an AIN, you have a reference to IDENTIFIED data. Claim 51, in sharp contrast, requires that the second database includes (1) de-identified data, and (2) an index—the person operating the second database does NOT have any means for associating the ID with a person. Claim 51 requires that the third database provides the anonymous ID, not the first database (thus, the operator of the first database with the identified data does NOT have any means to know the user's anonymous ID. Claim 51 requires that the first database provide de-identified data to a second database. In complete contrast to claim 51, Iliff shows a user interacting with a computer bank with the user's identification protected by a simple PIN or AIN (see column 75). Iliff provides no means to secure the patient's identity from the operator of the MDATA system.

52. A method of authenticating an anonymous user of a World-Wide-Web (WWW) site residing on a web server, said user requiring a web ID and a password to log on to said WWW site, said method comprising the steps:	Iliff shows an MDATA system where a known user (not an anonymous user) of web site interacts with the MDATA system. Figure 25a shows the user being able to interact using a variety of different communications devices, and shows the patient's medical and other records stored on one or more servers. Column 75 of Iliff clearly discloses the known user interacts by providing his PIN or AIN (in the case where a patient assistant is contacting the site).
verifying the true identity of said anonymous user on a registration authority server;	Iliff does not use a registration authority server. Column 75 clearly teaches that the user registers directly with the MDATA system and is assigned a PIN or an AIN.
creating said web ID on said web server, said web server including de-identified personal information including medical information of said user; and	Iliff does not use a web server to create a web ID. In Iliff, the patient's ID is not anonymous. It is known by the web server, and the protection scheme is a simple PIN or AIN system where the web server is able to authenticate the user—in all cases the MDATA system knows exactly who is contacting it by virtue of the PIN, i.e., the MDATA system knows everything–the patient ID and the patient information.

creating said password on a certificate authority server;	Iliff does NOT show or suggest a certificate authority server. Claim 52 requires a web ID to be created at the web server, and the password to be created at the certificate authority server. In sharp contrast, Iliff merely shows a registration system where a patient is registered and assigned a PIN or an AIN.
wherein said registration authority server, said web server, and said certificate authority server are operated separately from each other to preserver anonymity of said user, whereby the only party which knows the true identity, web ID and password of the user is the user.	Iliff does not show this feature. In Iliff both the MDATA system and the user know the PIN or AIN. In sharp contrast, claim 52 requires that ONLY the user knows the web ID and the password. This is accomplished by using both a certificate authority server and a web server.
53. The method according to claim 52 wherein on subsequent log ins to the WWW site by said user said password is authenticated by said certificate authority server and said Web ID is authenticated by said Web server.	This is NOT shown in Iliff. In Iliff, the user logs in using his PIN or AIN. At no point does Iliff show the use of both a certificate authority service and a web server. Furthermore, the system in Iliff is NOT anonymous. Rather, in Iliff, the MDATA system knows exactly who is logging in (by virtue of the PIN or AIN) and knows all of the data associated with that patient (i.e., there is no de-identified data)

In view of the foregoing, it is respectfully requested that the application be reconsidered, that claims 51-53 be allowed, and that the application be passed to issue.

Should the Examiner find the application to be other than in condition for allowance, the Examiner is requested to contact the undersigned at the local telephone number listed below to discuss any other changes deemed necessary in a telephonic or personal interview.

A provisional petition is hereby made for any extension of time necessary for the continued pendency during the life of this application. Please charge any fees for such provisional petition and any deficiencies in fees and credit any overpayment of fees to Attorney's Deposit Account No. 50-2041.

Respectfully submitted,

Michael E. Whitham
Reg. No. 32,635

Whitham, Curtis, Christofferson & Cook, P.C.
11491 Sunset Hills Road, Suite 340
Reston, VA 20190

Tel. (703) 787-9400
Fax. (703) 787-7557

Customer No.: 30743